BEST AVAILABLE COPY

RECEIVED
CENTRAL FAX CENTER

SEP 18 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: DOLEV, Moshe

Serial No. : 10/630,916

Filed : July 31, 2003

For : METHOD AND ASSEMBLY TO PREVENT IMPACT-DRIVEN MANIPULATION OF CYLINDER LOCKS

Group Art Unit 3676
Examiner: GALL, Lloyd A
Tel Aviv, Israel
September 14, 2006

Hon. Commissioner of Patents and Trademarks
Alexandria, VA 22313

Sir:

DECLARATION UNDER 37 CFR SEC 1.132

I, the undersigned, Moshe Dolev, of Rehov Bereishit 17, Ramat Hasharon, Israel 47201 hereby declare as follows:

Background Information

1. As the inventor, I am the owner and General Manager of Dolev Product Development, Raanana, Israel, which I established in 1987.

2. I have previously been employed by the following Israeli companies:

a) El Al Israel Airlines - tool maker and aircraft structure mechanic (12 years)
b) Founder and co-owner of Mul-T-Lock Ltd. (1973-1987), an internationally-recognized leader in door lock equipment;

3. My educational qualifications are summarized as:
Israel Military Industries High School for training in toolmaking (1955-1959)
Mechanic's Course - Heavy Maintenance of Aircraft (1964)
Business Management - Israel Management School (1979)

4. I am the inventor or co-inventor of approx. 30 published US patents and patent applications filed worldwide, dealing with locks and hair removers.

Overview Statements

5. The explanations contained in the following paragraphs address the uniqueness of the present invention over prior art solutions. The explanations do not replace the detailed background and technical details that were already provided in the patent application. These explanations are brought here to challenge the relevance of the Examiner's rejection statements, as stated in the Office Action (OA) dated March 23, 2006.

6. The present invention discloses a method and assembly for preventing unauthorized manipulation of common cylinder locks, using the Bumpkey or Blowgun methods, or any other method that is based on the principles of the impact and momentum phenomenon.

7. As stated in the Background section of the invention specification, the Bumpkey is a burglary tool, using an impact-driven blow for manipulation of cylinder locks. The technique was first developed in Denmark a quarter century ago, in the decade beginning with 1980 (see para. 12), based on an underlying theory of physics presented by Sir Isaac Newton over three centuries ago.

8. Impact-driven manipulation of cylinder locks, known also as the "Bumpkey" technique, is not known to many manufacturers of cylinder locks, and there has been limited activity in solving this problem.

9. Impact-driven manipulation of cylinder locks is a new technique using an old phenomenon, the physics of impact momentum. The Examiner has cited only one patent dealing with the subject, Stemmerick, issued in the US in January, 2004.

10. I participated in an international fair devoted to lock technology, in March 2004, in Cologne, Germany, and also in July, 2004 in Baltimore, MD. At these fairs, I demonstrated a working model which I constructed, showing the Bumpkey technique. Those in attendance who witnessed the demonstration responded with both amazement and shock at the simplicity of the technique and the danger it presents to lock security.

11. I have researched the Internet for articles dealing with the problem of the Bumpkey technique. Attached to this affidavit are five articles (each marked 1-5) which have been published on the Internet, describing this technique. At a recent Las Vegas conference entitled Defcon, "hackers" demonstrated the latest techniques in security fraud, including the Bumpkey technique.

12. In the article dated August 7, 2005 (marked "1"), a photo is shown of Mr. Marc Tobias, a lawyer and legal investigator, demonstrating the Bumpkey technique. He stated in a security

PAGE 2/14 * RCVD AT 9/18/2006 5:10:10 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-3/1 * DNIS:2738300 * CSID: * DURATION (mm-ss):05-16

seminar, in May 2006, that the Bumpkey technique is only around since approx. 1980 (see article marked "2").

13. The Bumpkey technique was demonstrated to the Examiner by my attorney, Mr. Edward Langer, in an interview conducted on March 8, 2005. Using this technique, Mr. Langer successfully opened a cylinder lock without using the lock key; instead, the Bumpkey technique was used.

14. On October 31, 2005, I demonstrated the Bumpkey technique to the Examiner, for a second time, using a large-scale model of a cylinder, and I also presented him with a CD showing, in slow motion, the internal operation of the pin assembly during Bumpkey manipulation.

My comments

15. In the previous Office Actions of February 17, 2005, July 18, 2005, and March 23, 2006, the Examiner has cited the Stemmerik patent for its teaching of a modified pin assembly which prevents "picking of the lock with an impact tool".

16. It is important to note that the use of the term "picking" in the above statement is misleading; if the intention is to indicate "opening of the lock with an impact tool", then the intention is understood. However, the term "picking" refers specifically to a technique related to the use of a back and forth jiggling motion on each pin, against the spring pressure, until the shear line is sensed.

17. Although stated previously, in the Response to the Office Action filed May 17, 2005, it is worthy of repetition, that the Stemmerik reference contains an inaccurate description of the physical nature of the impact and its result. Stemmerik states at col. 1, line 65:

"the stroke towards the tumbler pin is transmitted to the driver pin which is thereby lifted without any actual movement of the tumbler pin. By the arrangement according to the invention, the effect of the impact is transmitted through the movable member which constitutes one part of the driver pin".

At col. 3, line 13 he states:

"The member 11 in contact with the tumbler pin does not move....."

The reason these statements are incorrect is that the same physical forces which act on one pin act on the other, and cause them both to move. This was shown in the CD presented to the Examiner on October 31, 2005 (see above para. 14).

PAGE 3/14 * RCVD AT 9/18/2006 5:10:10 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-3/1 * DNIS:2738300 * CSID: * DURATION (mm-ss):05-16

18. My invention specification correctly describes the response to the impact in relation to Figs. 18-19, from p. 12, line 4 though p. 13, line 25:

(p. 12, line 5) "immediately after the hammer 62 has struck the Bumpkey 60 … both the tumbler pins and the driver pins (emphasis added) move from their locking positions …".

19. Since the Stemmerik statement is incorrect, it cannot reveal the approach of the present invention.

20. Further, Stemmerik contradicts himself in the description of the response to the impact energy, where he states at col. 3, line 28:

"To increase the security against the member 11 moving in spite of the impact energy being transmitted to the movable member 10, the member 11 may have a closer tolerance (tighter fit) in the associated bore than that of the remaining driver pins. In this way a friction between this driver pin and the bore is ensured."

21. Thus, Stemmerik at first states that the member 11 does not move, and then he later states that friction with the bore is needed to ensure this.

22. My invention does not rely on friction with the pins to achieve its goal, whereas Stemmerik does rely on this friction.

23. Stemmerik does not disclose a "motion alteration means adapted so as to alter the magnitude of its response to an impact-driven blow applied to said tumbler pin…"

24. For these reasons alone, Stemmerik is inappropriate as a reference teaching.

25. The Examiner has cited the Steinbach or Bessim patents, each for its teaching of a modification of the strength of the biasing springs in a pin tumbler lock to optimize its effectiveness against picking of the lock.

26. The Steinbach patent describes a cylinder lock manipulation technique by which the spring pressure strength is sensed in relation to the pin tumbler length. Since shorter pin tumblers have a longer extended spring (less compressed), this pressure can be sensed and translated into the tumbler pin length for purposes of preparing an illegal key. The Steinbach solution is to provide a set of tumbler and driver pins of uniform combined length, to make it impossible to sense different spring strengths. In addition, to mislead an intruder, Steinbach suggests providing at least two springs of different strength, to give the "wrong" information.

PAGE 4/14 * RCVD AT 9/18/2006 5:10:10 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-3/1 * DNIS:2738300 * CSID: * DURATION (mm-ss):05-16

27. Since the Steinbach patent was filed in 1978, he could not have related to the problem presented by the Bumpkey technique, which was not known prior to 1980. Therefore, the use by Steinbach of different spring strengths against the spring strength sensing technique cannot be a motivation to use this type of modification against an impact-driven manipulation, which was unknown at that time. Clearly, Steinbach does not suggest the use of different spring strengths as a way of interfering with impact-driven response, a response he could not have contemplated. Thus, Steinbach does not provide motivation for the impact case.

28. The Bessim patent, filed in 1970, describes a lock having a master key and a secondary key, allowing two degrees of locking safety. As with Steinbach, the impact-driven manipulation technique was not known at that time, so that there is no basis for suggesting that Bessim provides motivation for an impact case.

29. The Examiner has cited the Raskevicius and Surko patents, each for its teaching of a magnetic interlock between a driver and a tumbler pin to optimize its effectiveness against picking of the lock.

30. The Raskevicius patent, filed in July 1978, describes a "picking" technique by which the normal manufacturing tolerances of a cylinder lock are exploited, so that the driver pins are manipulated so as to clear the shear line while a rotational torque is maintained on the lock barrel portion. Another technique involves use of a key for jiggling the lock pins to give the same result. The solution proposed by Raskevicius is to provide a magnetic interlock between the driver and the key pin to prevent the driver pin from hanging up (getting stuck) on the shear line, and the key pin from dropping below the shear line, in certain lock-picking operations.

31. Since the Raskevicius patent was filed in 1978, he could not have related to the problem presented by the Bumpkey technique, which was not known prior to 1980. Thus, the use by Raskevicius of a magnetic interlock is not a motivation to use this type of modification against an impact-driven manipulation. Raskevicius does not provide motivation for the impact case.

32. The Surko patent, filed in 1976, describes a cylinder lock having a pin tumbler and driver releasably coupled together by mechanical means, when the cylinder lock is in a locked position. This type of cylinder lock is totally not susceptible to a Bumpkey technique. In addition, because it was filed in 1976, when the Bumpkey technique was not known, the use by Surko of magnetic means cannot provide any motivation to use this type of modification against an impact-driven manipulation.

PAGE 5/14 * RCVD AT 9/18/2006 5:10:10 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-3/1 * DNIS:2738300 * CSID: * DURATION (mm-ss):05-16

33. Thus, it would not have been obvious to one of ordinary skill in the art to have modified the pin assemblies via the biasing springs, or magnetic properties, for the impact case, as the Examiner maintains.

34. Therefore, prior art knowledge about biasing springs and magnetic properties, as applied to pin assembly modifications, does not make it "obvious to one of ordinary skill in the art" to modify the pin assemblies for the impact case.

35. Therefore, it is absolutely impossible that one of ordinary skill in the art would conclude, using the cited references to Steinbach, Bessim, Raskevicius or Surko, that it is obvious to modify the pin assemblies as a way of interfering with impact-driven response. None of these patents provides motivation.

36. In summary, the following conclusions may be drawn:

- the Bumpkey method of lock manipulation is a serious problem;
- "picking" is a misleading term as related to an impact tool;
- Stemmerick contradicts himself in describing the pin assembly response to the impact energy of the manipulation method;
- my invention does not rely on friction, whereas Stemmerik does rely on this friction;
- Stemmerik does not alter the response of the pin to an impact-driven blow;
- Steinbach and Bessim do not relate to impact-driven response;
- Raskevicius or Surko do not relate to impact-driven response.

37. This declaration is given in support of the patent prosecution efforts in the present application, before the USPTO.

38. I declare that all the statements made herein of my own knowledge are true, and that all statements made on information and knowledge are believed to be true, and further that these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Sec. 1001 of Title 18 of the United States Code, and the willful false statements may jeopardize the validity of the application and any patent issuing thereon.

Signed this 14 day of SEPTEMBER 2006.

M. DOLEV

Moshe Dolev

PAGE 6/14 * RCVD AT 9/18/2006 5:10:10 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-3/1 * DNIS:2738300 * CSID: * DURATION (mm-ss):05-16

CNN INTERNATIONAL .com Member Center: Sign In | Register

GIVE YOUR FINGERS A REST.

SEARCH THE WEB CNN.com SEARCH Powered by YAHOO!

Home Page
Asia
Europe
U.S.
World
World Business
Technology
Science & Space
Entertainment
World Sport
Travel
Weather
Special Reports
Video
CNN Exchange
ON TV
CNN Pipeline
What's On
Art of Life
Business Traveller
Future Summit
Principal Voices
Quest
Revealed
Talk Asia
Services
Languages

TECHNOLOGY

Researcher: New passports vulnerable

Defcon showcases latest discovered security weaknesses

Monday, August 7, 2006 Posted: 0004 GMT (0804 HKT)

LAS VEGAS, Nevada (AP) – Electronic passports being introduced in the United States and other countries have a major vulnerability that could allow criminals to clone embedded secret code and enter countries illegally, an expert warned.

A demonstration late Friday by German computer security expert Lukas Grunwald showed how personal information stored on the documents could be copied and transferred to another device.

It appeared to contradict assurances by officials in government and private industry that the electronic information stored in passports could not be duplicated.

"If there is an automatic inspection system, I can use this card to enter any country," Grunwald said, holding up a computer chip containing electronic information he had copied from his German passport.

The research is the latest to raise concerns about the growing use of RFID, short for radio-frequency identification, which allows everyday objects such as store merchandise, livestock and security documents to beam electronic data to computers equipped with special antennas.

Countries such as Germany already use RFID in passports to help border officials guard against forgeries and automate the processing of international visitors. U.S. officials plan to start embedding RFID in passports in October.

A State Department spokeswoman said late Saturday she did not have enough information on the matter to comment.

The presentation was one of dozens delivered at the Defcon conference being held

Marc Tobias demonstrates a technique for secretly picking locks.

RELATED See p-2

• Is RFID tracking you?

YOUR E-MAIL ALERTS

Computer Security
Computing and Information Technology
Defcon

ACTIVATE or Create Your Own

Manage Alerts | What Is This?

advertisement
Your E-Mail Ale
Travel the Worl
CNNarabic.com
Sports Update

through Sunday in Las Vegas. The conference, attended by many of the world's best-known security experts, has become an annual showcase of the latest discovered weaknesses in computers, phone equipment and other machines.

Routers faulted

Another security professional showed how people can have their phone numbers hijacked when using certain types of equipment that route calls over the Internet.

The research, from Arias Hung, a security professional with Media Access Guard in Seattle, showed how to control the inner workings of Internet phone routers made by Linksys, which is owned by Cisco Systems Inc.

Once the routers are accessed, a person can change the device's so-called media access control address, which acts as a serial number that Internet phone providers such as Vonage Holdings Corp. use to verify the identity of customers.

A person exploiting the flaw could intercept calls made to a legitimate Vonage user and make calls that would appear to come from the user's phone number.

"The service providers should be very concerned," Hung said. "The general consumer should stay away from this router," he said, referring to two models that Linksys designates the WRTP54G and the RTP300.

Cisco spokeswoman Molly Ford said she could not immediately comment on Hung's research.

Although Defcon focuses largely on computers, not all the research focused on circumventing high tech gizmos.

Marc Tobias, a South Dakota lawyer who authored a textbook for locksmiths, showed how a simple technique can allow a person to secretly pick the locks of most homes, businesses and post office mailboxes.

The method, known as bumping, requires a person to file down a key and then gently tap it into a lock.

"You can do this with virtually every lock," said Tobias, who is calling for a change to U.S. postal regulations to prohibit the trafficking of bump keys, which are advertised for sale on the Internet.

Copyright 2006 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten, or redistributed.

Story Tools
SAVE THIS E-MAIL THIS
PRINT THIS MOST POPULAR

advertisement
Click Here to try 4 Free Trial Issues of Time!

SCI-TECH
Section Page · Video · Business 2.0

Feeling blue? So will your artwork

• **CNNMoney:** AOL to slash 5,000 jobs
• Review: Chill out with cool Nintendo DS games
• Microsoft to hackers: Take your best shot

TOP STORIES
Home Page · Video · Most Popular

Bloodshed in Mideast

• Alaska oil field shuts after spill
• Iraq rape-kill detailed in court
• Aid worker deaths: Rebels blamed

CNN U.S. Languages CNN TV E-mail Services CNN Mobile CNNAvantGo CNNtext Ad Info

PAGE 8/14 * RCVD AT 9/18/2006 5:10:10 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-3/1 * DNIS:2738300 * CSID: * DURATION (mm-ss):05-16

UNIVERSITY OF CAMBRIDGE

Security Seminar
23 May 2006: Marc Weber Tobias, Investigative Law Offices

SECURITY SEMINAR SERIES

Title: Opening locks by bumping in five seconds or less: is it really a threat to physical security?

Speaker: Marc Weber Tobias, Investigative Law Offices

Date: Tuesday, 23 May 2006, 14:15

Place: Lecture Theatre 2, William Gates Building

2

bstract:

here are millions of pin tumbler locks in the world that provide the primary security for the onsumer, business and government. The vast majority of these can be compromised in seconds ith a minimal skill level and virtually no tools. The procedure is called "bumping" and was first eveloped in Denmark a quarter century ago, although the underlying theory of physics was in fact resented by Sir Isaac Newton over three centuries ago. Marc Weber Tobias presents an troduction to the technique of bumping and a detailed analysis of its real security threat.

(approx. 1980)

resentation slides (Powerpoint, 8.2M)

) 2006 University of Cambridge Computer Laboratory
lease send any comments to Stephen Lewis
age last updated on 25-May-2006 at 17:05 by Stephen Lewis

(mwtobias@security.org)
Marc Weber Tobias

CTV.ca SEARCH The Web CTV.ca
Home | NEWS | Canada AM | Weather | Sports | Entertainment | Programs | TV Listings | Contests
CTV NEWS
Get live breaking news on your des
Sign up for live streaming video of CTV Ne
Latest News: Israe_
NEWS Programs CTV News Team Services
Top Stories Canada World Entertainment Health Sports Business SCI-TECH Politics Consumer

Sci-Tech

If passports such as the one pictured here are phased out in favour of electronic idenfication, experts fear they could be hacked and used by terrorists.

Electronic passports vulnerable, expert says

Updated Sun. Aug. 6 2006 7:45 PM ET

Associated Press

LAS VEGAS -- Electronic passports being introduced in the United States and other countries have a major vulnerability that could allow criminals to clone embedded secret code and enter countries illegally, an expert warned.

A demonstration late Friday by German computer security expert Lukas Grunwald showed how personal information stored on the documents could be copied and transferred to another device.

It appeared to contradict assurances by officials in government and private industry that the electronic information stored in passports could not be duplicated.

"If there is an automatic inspection system, I can use this card to enter any country," Grunwald said, holding up a computer chip containing electronic information he had copied from his German passport.

The research is the latest to raise concerns about the growing use of RFID, short for radio-frequency identification, which allows everyday objects such as store merchandise, livestock and security documents to beam electronic data to computers equipped with special antennae.

Countries such as Germany already use RFID in passports to help border officials guard against forgeries and automate the processing of international visitors. U.S. officials plan to start embedding RFID in passports in October.

The presentation was one of dozens delivered at the Defcon conference being held through Sunday in Las Vegas. The conference, attended by many of the world's best-known security experts, has become an annual showcase of the latest discovered weaknesses in computers, phone equipment and other machines.

RELATED STORIES
- U.S. proposes fingerprinting Canadian workers
- High-tech passport system eyed for Canadians

USER TOOLS
- Print This Page
- E-Mail Story
- Feedback

3

See p-2

Ads by
Marke soluti Integr to con RFID requir www.m
RFID and C Free, and a indep exper www.id
Intelli The le suppli RFID soluti www.in
RFID Manu Samp availa 13.56 low pr www.vz
Adverti

PAGE 10/14 * RCVD AT 9/18/2006 5:10:10 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-3/1 * DNIS:2738300 * CSID: * DURATION (mm-ss):05-16

Another security professional showed how people can have their phone numbers hijacked when using certain types of equipment that route calls over the Internet.

The research, from Arias Hung, a security professional with Media Access Guard in Seattle, showed how to control the inner workings of Internet phone routers made by Linksys, which is owned by Cisco Systems Inc. of San Jose, Calif.

Once the routers are accessed, a person can change the device's so-called media access control address, which acts as a serial number that Internet phone providers such as Vonage Holdings Corp. use to verify the identity of customers. A person exploiting the flaw could intercept calls made to a legitimate Vonage user and make calls that would appear to come from the user's phone number.

"The service providers should be very concerned," Hung said.

"The general consumer should stay away from this router," he said, referring to two models Linksys designates the WRTP54G and the RTP300.

Cisco spokeswoman Molly Ford said she could not immediately comment on Hung's research.

Although Defcon focuses largely on computers, not all the research focused on circumventing high-tech gizmos.

Marc Tobias, a South Dakota lawyer who authored a textbook for locksmiths, showed how a simple technique can allow a person to secretly pick the locks of most homes, businesses and post office mailboxes.

The method, known as bumping, requires a person to file down a key and then gently tap it into a lock.

"You can do this with virtually every lock," said Tobias, who is calling for a change to U.S. postal regulations to prohibit the trafficking of bump keys, which are advertised for sale on the Internet.

USER TOOLS
Print This Page
E-Mail Story
Feedback

SCITECH STORIES
- Electronic passports vulnerable, expert says
- Your boss can now track you on your cell phone
- Indonesia rebels cash in on risky logging binge
- 10 years later, few believe in life on Mars
- Your cell phone could be home to nasty bacteria
- Canadian astronaut eager to fly in Shuttle
- X-ray beam reveals ancient Archimedes' writings
- Ship hits pier, spilling oil north of Vancouver
- Philippines officials warn volcano may erupt

PAGE 11/14 * RCVD AT 9/18/2006 5:10:10 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-3/1 * DNIS:2738300 * CSID: * DURATION (mm-ss):05-16

Chevron is one of the companies mentioned. Chevron's corp network was compromised to send out large amounts of spam. Indeed, why would you bother with pesky home desktops, if you can compromise a large corp network hooked up to a T1.

Posted in DefCon | No Comments »

DefCon Chronicles: why DefCon is unique

Sunday, August 6th, 2006

DefCon is probably the only conference where

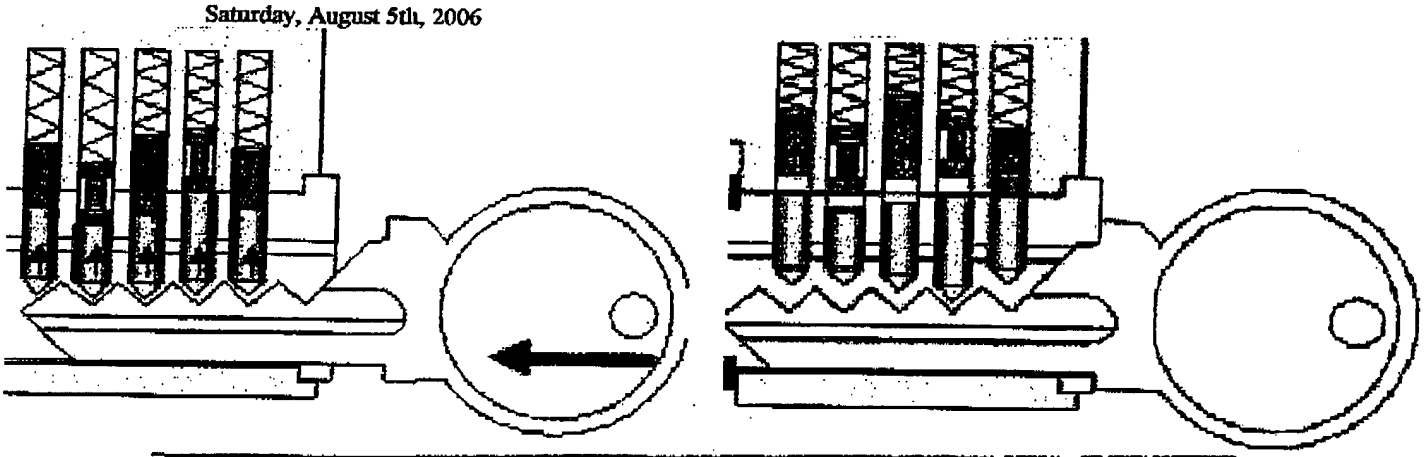
1. the organizers keep reporting on dealing with hotel management, and whether or not the conference will be kicked out (fyi, Riviera is quite happy with DefCon attendees so far)
2. the early 10 am speaker brings helpings of beer to his talk just to help people who are hungover

4

Posted in DefCon | No Comments »

DefCon Chronicles: open any lock under 5 seconds

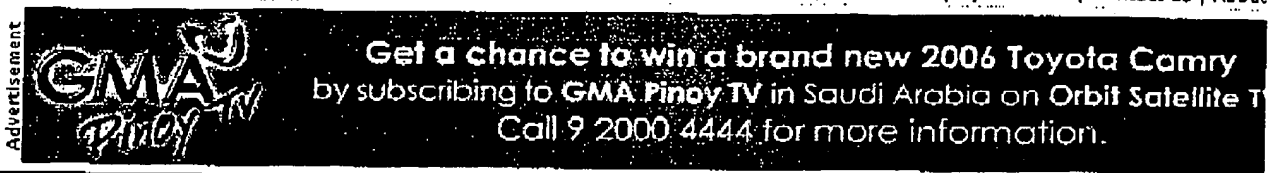
Saturday, August 5th, 2006



Marc Weber Tobias and **Matt Fiddler** are talking about bump-opening most of the locks out there in the United States. The full paper is availavle at security.org. They also conducted a research with USPS and Mailboxes, etc. While USPS quickly worked with the researchers and agreed that the issue was there, MailBoxes, etc. keeps denying there's a problem. A PDF with detailed technical analysis is also available. The presentation promised:

> Case examples and demonstrations detailing a major security flaw and vulnerability in locks used by the federal government and a private sector corporation that affect millions of users will be presented.

and it certainly delivered that. Live in an apartment complex? you can make a **bump key** out of your key that will open any apartment. Rent a mail box? Gain access to anything that uses the same type of key. And if you're bothered too much with creating your own bump keys, just buy some off eBay.

Advertisement


Advertisement


GMA7 TV-RADIO
08/07/2006
Mt. Mayon, posibleng magkaroon ng major eruption ngayong araw

i-GMA.tv
Join DEBATE POLL
GMA7 dzBB

SPECIAL REPORT

Breaking News / World

5

Lock picking child's play at hackers conference

Agence France-Presse
Last updated 09:46am (Mla time) 08/07/2006

LAS VEGAS -- Locks commonly used at homes and businesses worldwide were so easy to pick that children could do it, computer hackers practicing the skill were shown on Sunday.

In a Las Vegas casino meeting room devoted to the art of lock picking for the course of a three-day DefCon hackers conference, Marc Tobias and Matt Fiddler demonstrated that all it took to open a lock was a tap and a twist.

Emphatic proof arrived in the form of an 11-year-old girl, who deftly opened typical door locks under the watchful eyes of her mother within minutes of being given a "bump key" and a brief lesson in how to use it.

"That was absolutely my coup," said Tobias, a lawyer and a security consultant that authored Locks, Safes and Security. "I'm putting her picture on my website, along with a video of her doing it."

The type of bump key used by the girl was developed in Denmark long ago and basically was an easily modified key blank, Tobias explained.

Putting bump keys in typical pin tumbler locks and giving them a whack sent shock waves that jarre position for opening, Tobias showed Agence France-Presse.

"My old friend Isaac Newton 350 years ago figured out bumping," Tobias said, likening it to the princ action having an equal and opposite reaction. "It is just that there were no locks with pins in them."

"It's a very simple premise."

Tobias began calling attention to the vulnerability in the United States about two years ago, after col same in The Netherlands.

The technique could be used to open almost any lock, from weighty ones used by urban merchants down gates to home door locks and those on the approximately five million US post office boxes, T

ARTICLE SERVICES
Reprint this article
Print this a
Send as an e-mail
Feedback

RELATED STORIES
Roundup
CHR probes alleged torture of Iloilo farme
Makati jail inmates complete IT training

Advertisement

OTHER STORIES
Singapore urges regional security coopers
China's death toll from 'Prapiroon' rises to
Lock picking child's play at hackers confer
15 killed by Hezbollah rockets on Israel's t

More Stories »

ARTICLE SERVICES
Reprint this article
Print this a
Send as an e-mail
Feedback

SUBSCRIBE TO INQ7eXTI

PAGE 13/14 * RCVD AT 9/18/2006 5:10:10 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-3/1 * DNIS:2738300 * CSID: * DURATION (mm-ss):05-16

Pedicab man returns bag with P104,000

More Sites: State of Emergency, Leyte Landslide, ULTRA Stampede, The Pacquiao Files, Edsa 20

INQ7 ALERT
Get the free INQ7 newsletter
Enter your email address:

LOTTO

2 Digit Result: 08 19
3 Digit: 3 2 3
Super Lotto 6/49
Winning Numbers:
39 46 24 20 49 18
P21,887,503.20

CITYGUIDE

Search the city for:
GO
Powered by:
ClickTheCity.com

Affiliates

Agence France-Presse.

"These locks are all over the world," Tobias said. "There isn't a lock in France I can't open."

A few companies such as EVVA of Austria make far more secure locks based on sliders or magnets pins, according to Fiddler and Tobias, who opted for those kinds of locks on their homes.

"The problem is that the public doesn't get it," Fiddler said. "They don't know, and the lock manufact want to tell them."

Tobias, a lawyer who began picking locks for fun at the age of 15, joked that all he wanted was for p packaging to bear warnings that the devices could be opened by people with little skill using basic to

"It is inherent in the pin tumbler lock," Tobias said. "If you have real security needs, buy better locks

Lock picking held an allure for computer hackers, more than 6,000 of which turned out for the 14th a conference that ended on Sunday in Las Vegas, according to organizers.

They were curious about how things worked, and then took pride in figuring out how to crack codes software barriers, attendees conceded.

Hackers crammed the room each day to hone lock-picking skills or compete for the title of top lock-p

"I was completely dumbfounded that this was possible," DefCon attendee Tom Lappas told Agence as he practiced bumping a lock. "I thought you needed a sledge hammer and chain saw to do this."

"The existence of a room full of people doing this is astounding."

It was vital to know what security could be breached, whether it was a door lock or a computer prog build better defenses, said the 24-year-old California university student.

The US Postal Service was taking action to make post office boxes more secure, and efforts were u address the bump key vulnerability in Europe, according to Tobias and Fiddler.

"They are dealing with it in Europe," Tobias said. "The problem is there are a billion locks out there.'

Copyright 2006 Agence France-Presse. All rights reserved. This material may not be publish rewritten or redistributed.

RELATED STORIES:
Roundup
CHR probes alleged torture of Iloilo farmers
Makati jail inmates complete IT training

OTHER STORIES:
Singapore urges regional security cooperation
China's death toll from 'Prapiroon' rises to 77
Lock picking child's play at hackers conference
15 killed by Hezbollah rockets on Israel's bloodiest day

© Copyright 2001-2006 INQ7 Interactive, Inc. An INQUIRER and GMA Network Company

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.